UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/259,991	03/01/1999	CHRIS W. MAHNE	240/218	5948

7590 11/20/2002

SOCAL LP LAW GROUP
310 N. WESTLAKE BLVD.
SUITE 120
WESTLAKE VILLAGE, CA 91362

EXAMINER
SMITHERS, MATTHEWS

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/20/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/259,991	Applicant(s) MAHNE ET AL.	
	Examiner Matthew B Smithers	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 September 2002* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *47-79* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *47-79* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Status of Application

On October 10, 2001, an error was made in sending a notice of abandonment to the applicant. Applicant's petition to revive the abandoned case was granted on July 30, 2001. The examiner did not fully consider the granted petition at the time of submitting the notice of abandonment. After further reviewing the grant of the petition by the Office of Petitions, the examiner's next office action was in response to the amendment, paper #8, submitted along with the petition. The office action below will address the latest amendment, paper #18, given by applicant.

Response to Arguments

Applicant's arguments with respect to claims 47-77 have been considered but are moot in view of the new ground(s) of rejection. A new rejection is given below on claims 47-79.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 60-66, 68-73, and 76-79 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. patent 5,584,023 granted to Hsu and further in view of U.S. patent 6,249,866 granted to Brundrett et al.

Regarding claim 60, Hsu teaches a computer system that uses a transparent file transform mechanism for encrypting and decrypting files (see column 3, line 14 to column 4, line 26 and column 6, line 1 to column 18, line 7). Hsu's preferred embodiment uses a file-oriented paradigm in providing the operating services on a UNIX operating system (see column 5, lines 46-48 and column 6, lines 44-45). The file transform mechanism provides transparent encryption/decryption services after receiving a change command to act on the file (see column 16, line 50 to column 17, line 39 and Figure 5B.) Hsu fails to specifically teach selecting an algorithm from a plurality of algorithms to use on the file and validating (verifying) the encrypted data identifier. Brundrett teaches a file encryption system in which a user is allowed to select an algorithm from a plurality of algorithms and to encrypt using the selected algorithm (see column 10, lines 54-66). Brundrett also teaches validating (verifying) the integrity of the encrypted data (see column 16, lines 12-22). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Brundrett's file encryption system with Hsu's computer system with transparent file transform services in order to provide the encryption system with the flexibility of selecting algorithms in accordance with the user's needs for a particular file [see **Brundett et al**; column 1, line 63 to column 2, line 3].

Regarding claim 61, Hsu and Brundrett et al disclose everything claimed as applied above, (see claim 60) in addition Hsu teaches selecting a file from within another file (see column 6, line 1 to column 18, line 7).

Regarding claim 62, Hsu and Brundrett et al disclose everything claimed as applied above, (see claim 61) in addition Hsu teaches encrypted file located in a container (disk inode entries) (see column 6, lines 44-56).

Regarding claim 63, Hsu and Brundrett et al disclose everything claimed as applied above, (see claim 62) in addition Hsu teaches creating a file containing the encrypted file and a portion of the second file that does not include the file (see column 6, lines 44-56).

Regarding claim 64, Hsu and Brundrett et al disclose everything claimed as applied above, (see claim 63) in addition Hsu teaches a third file (disk inode entries) (see column 6, lines 44-56).

Regarding claim 65, Hsu and Brundrett et al disclose everything claimed as applied above, (see claim 64) in addition Hsu teaches decryption by an appropriate method (see column 12, lines 45-49).

Regarding claim 66, Hsu and Brundrett et al disclose everything claimed as applied above. (see claim 64) in addition Hsu teaches recreating the second file after decrypting the file (see column 6, lines 44-56 and column 11, line 25 to column 16, line 49).

Regarding claim 68, Hsu teaches a computer system that uses a transparent file transform mechanism for encrypting and decrypting files (see column 3, line 14 to

column 4, line 26 and column 6, line 1 to column 18, line 7). Hsu's preferred embodiment uses a file-oriented paradigm in providing the operating services on a UNIX operating system (see column 5, lines 46-48 and column 6, lines 44-45). The file transform mechanism provides transparent encryption/decryption services after receiving a change command to act on the file (see column 16, line 50 to column 17, line 39 and Figure 5B.) Hsu fails to specifically teach selecting an algorithm from a plurality of algorithms to use on the file and validating (verifying) the encrypted data identifier. Brundrett teaches a file encryption system in which a user is allowed to select an algorithm from a plurality of algorithms and to encrypt using the selected algorithm (see column 10, lines 54-66). Brundrett also teaches the validating (verifying) integrity of the encrypted data (see column 16, lines 12-22). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Brundrett's file encryption system with Hsu's computer system with transparent file transform services in order to provide the encryption system with the flexibility of selecting algorithms in accordance with the user's needs for a particular file [see **Brundett et al**; column 1, line 63 to column 2, line 3].

Regarding claim 69, Hsu teaches a computer system that uses a transparent file transform mechanism for encrypting and decrypting files (see column 3, line 14 to column 4, line 26 and column 6, line 1 to column 18, line 7). Hsu's preferred embodiment uses a file-oriented paradigm in providing the operating services on a UNIX operating system (see column 5, lines 46-48 and column 6, lines 44-45). The file transform mechanism provides transparent encryption/decryption services after

receiving a change command to act on the file (see column 16, line 50 to column 17, line 39 and Figure 5B.) Hsu's system provides services to users in an inter-networked environment (see column 3, lines 14-18). Hsu fails to specifically teach selecting an algorithm from a plurality of algorithms to use on the file and validating (verifying) the encrypted data identifier. Brundrett teaches a file encryption system in which a user is allowed to select an algorithm from a plurality of algorithms and to encrypt using the selected algorithm (see column 10, lines 54-66). Brundrett also teaches validating (verifying) the integrity of the encrypted data (see column 16, lines 12-22). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Brundrett's file encryption system with Hsu's computer system with transparent file transform services in order to provide the encryption system with the flexibility of selecting algorithms in accordance with the user's needs for a particular file [see **Brundett et al**; column 1, line 63 to column 2, line 3].

Regarding claim 70, Hsu and Brundrett et al disclose everything claimed as applied above, (see claim 69) in addition Hsu teaches an environment for inter-networked computer systems where a file (message) can be obtained by a user (see column 3, line 14 to column 4, line 26).

Regarding claim 71, Hsu teaches a computer system that uses a transparent file transform mechanism for encrypting and decrypting files (see column 3, line 14 to column 4, line 26 and column 6, line 1 to column 18, line 7). Hsu's preferred embodiment uses a file-oriented paradigm in providing the operating services on a UNIX operating system (see column 5, lines 46-48 and column 6, lines 44-45). The file

transform mechanism provides transparent encryption/decryption services after receiving a change command to act on the file (see column 16, line 50 to column 17, line 39 and Figure 5B). Hsu fails to specifically teach selecting an algorithm from a plurality of algorithms to use on the file and validating (verifying) the encrypted data identifier. Brundrett teaches a file encryption system in which a user is allowed to select an algorithm from a plurality of algorithms and to encrypt using the selected algorithm (see column 10, lines 54-66). Brundrett also teaches validating (verifying) the integrity of the encrypted data (see column 16, lines 12-22). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Brundrett's file encryption system with Hsu's computer system with transparent file transform services in order to provide the encryption system with the flexibility of selecting algorithms in accordance with the user's needs for a particular file [see **Brundett et al**; column 1, line 63 to column 2, line 3].

Regarding claim 72, Hsu and Brundrett et al disclose everything claimed as applied above, (see claim 71) in addition Brundrett teaches decrypting a portion of the file identifier before validating the decryption key value (see column 16, lines 12-22).

Regarding claim 73, Hsu and Brundrett et al disclose everything claimed as applied above, (see claim 72) in addition Brundrett teaches encrypting the file identifier before validating the decryption key value (see column 16, lines 12-22).

Regarding claim 76, Hsu teaches a computer system that uses a transparent file transform mechanism for encrypting and decrypting files (see column 3, line 14 to column 4, line 26 and column 6, line 1 to column 18, line 7). Hsu's preferred

embodiment uses a file-oriented paradigm in providing the operating services on a UNIX operating system (see column 5, lines 46-48 and column 6, lines 44-45). The file transform mechanism provides transparent encryption/decryption services after receiving a change command to act on the file (see column 16, line 50 to column 17, line 39 and Figure 5B.) Hsu fails to specifically teach selecting an algorithm from a plurality of algorithms to use on the file. Brundrett teaches a file encryption system in which a user is allowed to select an algorithm from a plurality of algorithms and to encrypt using the selected algorithm (see column 10, lines 54-66). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Brundrett's file encryption system with Hsu's computer system with transparent file transform services in order to provide the encryption system with the flexibility of selecting algorithms in accordance with the user's needs for a particular file [see **Brundett et al**; column 1, line 63 to column 2, line 3].

Regarding claim 77, Hsu teaches a computer system that uses a transparent file transform mechanism for encrypting and decrypting files (see column 3, line 14 to column 4, line 26 and column 6, line 1 to column 18, line 7). Hsu's preferred embodiment uses a file-oriented paradigm in providing the operating services on a UNIX operating system (see column 5, lines 46-48 and column 6, lines 44-45). The file transform mechanism provides transparent encryption/decryption services after receiving a change command to act on the file (see column 16, line 50 to column 17, line 39 and Figure 5B.) Hsu fails to specifically teach selecting an algorithm from a plurality of algorithms to use on the file and validating (verifying) the encrypted data

identifier. Brundrett teaches a file encryption system in which a user is allowed to select an algorithm from a plurality of algorithms and to encrypt using the selected algorithm (see column 10, lines 54-66). Brundrett also teaches validating (verifying) the integrity of the encrypted data (see column 16, lines 12-22). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Brundrett's file encryption system with Hsu's computer system with transparent file transform services in order to provide the encryption system with the flexibility of selecting algorithms in accordance with the user's needs for a particular file [see **Brundett et al**; column 1, line 63 to column 2, line 3].

Regarding claim 78, Hsu teaches a computer system that uses a transparent file transform mechanism for encrypting and decrypting files (see column 3, line 14 to column 4, line 26 and column 6, line 1 to column 18, line 7). Hsu's preferred embodiment uses a file-oriented paradigm in providing the operating services on a UNIX operating system (see column 5, lines 46-48 and column 6, lines 44-45). The file transform mechanism provides transparent encryption/decryption services after receiving a change command to act on the file (see column 16, line 50 to column 17, line 39 and Figure 5B.) Hsu fails to specifically teach selecting an algorithm from a plurality of algorithms to use on the file. Brundrett teaches a file encryption system in which a user is allowed to select an algorithm from a plurality of algorithms and to encrypt using the selected algorithm (see column 10, lines 54-66). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Brundrett's file encryption system with Hsu's computer system with transparent file

transform services in order to provide the encryption system with the flexibility of selecting algorithms in accordance with the user's needs for a particular file [see **Brundett et al**; column 1, line 63 to column 2, line 3].

Regarding claim 79, Hsu teaches a computer system that uses a transparent file transform mechanism for encrypting and decrypting files (see column 3, line 14 to column 4, line 26 and column 6, line 1 to column 18, line 7). Hsu's preferred embodiment uses a file-oriented paradigm in providing the operating services on a UNIX operating system (see column 5, lines 46-48 and column 6, lines 44-45). The file transform mechanism provides transparent encryption/decryption services after receiving a change command to act on the file (see column 16, line 50 to column 17, line 39 and Figure 5B.). Hsu fails to specifically teach selecting an algorithm from a plurality of algorithms to use on the file and validating (verifying) the encrypted data identifier. Brundrett teaches a file encryption system in which a user is allowed to select an algorithm from a plurality of algorithms and to encrypt using the selected algorithm (see column 10, lines 54-66). Brundrett also teaches validating (verifying) the integrity of the encrypted data (see column 16, lines 12-22). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Brundrett's file encryption system with Hsu's computer system with transparent file transform services in order to provide the encryption system with the flexibility of selecting algorithms in accordance with the user's needs for a particular file [see **Brundett et al**; column 1, line 63 to column 2, line 3].

Claims 47-59, 67, 74, and 75 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. patent 5,584,023 granted to Hsu and further in view of U.S. patent 6,249,866 granted to Brundrett et al and U.S. patent 5,815,571 granted to Finley.

Regarding claim 47, Hsu teaches a computer system that uses a transparent file transform mechanism for encrypting and decrypting files (see column 3, line 14 to column 4, line 26 and column 6, line 1 to column 18, line 7). Hsu's preferred embodiment uses a file-oriented paradigm in providing the operating services on a UNIX operating system (see column 5, lines 46-48 and column 6, lines 44-45). The file transform mechanism provides transparent encryption/decryption services after receiving a change command to act on the file (see column 16, line 50 to column 17, line 39 and Figure 5B.) Hsu fails to specifically teach selecting an algorithm from a plurality of algorithms to use on the file and a mechanism for invoking or running a virus scan program on the files executed within the computer system. Brundrett teaches a file encryption system in which a user is allowed to select an algorithm from a plurality of algorithms and to encrypt using the selected algorithm (see column 10, lines 54-66). Finley teaches a computer system in which user programs are executed in a location where embedded viruses can be detected transparent to the user (see column 3, line 51 to column 6, line 58). Finley teaches the security settings and the filter processors can be set by the operator. This allows the operator (user) the option to invoke security and/or filter settings (see column 5, lines 39-41). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Finley's method of protection within a computer system and Brundrett's file encryption system with Hsu's

computer system with transparent file transform services in order to prevent hackers from gaining access to the core operating system commands via embedded viruses [see **Finley**; column 1, lines 22-43] and to further provide the encryption system with the flexibility of selecting algorithms in accordance with the user's needs for a particular file [see **Brundett et al**; column 1, line 63 to column 2, line 3].

Regarding claim 48, Hsu, Brundrett et al and Finley disclose everything claimed as applied above, (see claim 47) in addition Finley teaches running a virus scan (see column 3, line 51 to column 6, line 58).

Regarding claim 49, Hsu, Brundrett et al and Finley disclose everything claimed as applied above, (see claim 47) in addition Hsu teaches selecting a file from within another file (see column 6, line 1 to column 18, line 7).

Regarding claim 50, Hsu, Brundrett et al and Finley disclose everything claimed as applied above, (see claim 49) in addition Hsu teaches creating a file containing the encrypted file and a portion of the second file that does not include the file (see column 6, lines 44-56).

Regarding claim 51, Hsu, Brundrett et al and Finley disclose everything claimed as applied above, (see claim 50) in addition Hsu teaches encrypted file located in a container (disk inode entries) (see column 6, lines 44-56).

Regarding claim 52, Hsu, Brundrett et al and Finley disclose everything claimed as applied above, (see claim 47) in addition Hsu teaches selecting an algorithm from pre-selected criteria (see column 11, line 25 to column 12, line 53).

Regarding claim 53, Hsu, Brundrett et al and Finley disclose everything claimed as applied above, (see claim 47) in addition Brundrett teaches selecting an algorithm from a preselected algorithm (see column 10, lines 54-66).

Regarding claim 54, Hsu, Brundrett et al and Finley disclose everything claimed as applied above, (see claim 47) in addition Hsu teaches inserting the file identifier according to a pre-selected criteria (see column 14, lines 41-58).

Regarding claim 55, Hsu, Brundrett et al and Finley disclose everything claimed as applied above, (see claim 47) in addition Hsu teaches inserting the file identifier according to a pre-selected algorithm (see column 14, lines 41-58).

Regarding claim 56, Hsu, Brundrett et al and Finley disclose everything claimed as applied above, (see claim 47) in addition Hsu teaches plural encryption key values an at least one associated with a user (see column 6, lines 44-56).

Regarding claim 57, Hsu, Brundrett et al and Finley disclose everything claimed as applied above, (see claim 56) in addition Hsu teaches an access authentication step (see column 14, line 59 to column 16, line 65).

Regarding claim 58, Hsu teaches a computer system that uses a transparent file transform mechanism for encrypting and decrypting files (see column 3, line 14 to column 4, line 26 and column 6, line 1 to column 18, line 7). Hsu's preferred embodiment uses a file-oriented paradigm in providing the operating services on a UNIX operating system (see column 5, lines 46-48 and column 6, lines 44-45). The file transform mechanism provides transparent encryption/decryption services after receiving a change command to act on the file (see column 16, line 50 to column 17,

line 39 and Figure 5B.) Hsu fails to specifically teach selecting an algorithm from a plurality of algorithms to use on the file and validating (verifying) the encrypted data identifier. Brundrett teaches a file encryption system in which a user is allowed to select an algorithm from a plurality of algorithms and to encrypt using the selected algorithm (see column 10, lines 54-66). Brundrett also teaches validating (verifying) the integrity of the encrypted data (see column 16, lines 12-22). Hsu also fails to specifically teach a mechanism for invoking or running a virus scan program on the files executed within the computer system. Finley teaches a computer system in which user programs are executed in a location where embedded viruses can be detected transparent to the user (see column 3, line 51 to column 6, line 58). Finley teaches the security settings and the filter processors can be set by the operator. This allows the operator (user) the option to invoke security and/or filter settings (see column 5, lines 39-41). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Finley's method of protection within a computer system and Brundrett's file encryption system with Hsu's computer system with transparent file transform services in order to prevent hackers from gaining access to the core operating system commands via embedded viruses [see **Finley**; column 1, lines 22-43] and to further provide the encryption system with the flexibility of selecting algorithms in accordance with the user's needs for a particular file [see **Brundett et al**; column 1, line 63 to column 2, line 3].

Regarding claim 59, Hsu teaches a computer system that uses a transparent file transform mechanism for encrypting and decrypting files (see column 3, line 14 to column 4, line 26 and column 6, line 1 to column 18, line 7). Hsu's preferred

embodiment uses a file-oriented paradigm in providing the operating services on a UNIX operating system (see column 5, lines 46-48 and column 6, lines 44-45). The file transform mechanism provides transparent encryption/decryption services after receiving a change command to act on the file (see column 16, line 50 to column 17, line 39 and Figure 5B. Hsu fails to specifically teach selecting an algorithm from a plurality of algorithms to use on the file and validating (verifying) the encrypted data identifier. Brundrett teaches a file encryption system in which a user is allowed to select an algorithm from a plurality of algorithms and to encrypt using the selected algorithm (see column 10, lines 54-66). Brundrett also teaches validating (verifying) the integrity of the encrypted data (see column 16, lines 12-22). Hsu also fails to specifically teach a mechanism for invoking or running a virus scan program on the files executed within the computer system. Finley teaches a computer system in which user programs are executed in a location where embedded viruses can be detected transparent to the user (see column 3, line 51 to column 6, line 58). Finley teaches the security settings and the filter processors can be set by the operator. This allows the operator (user) the option to invoke security and/or filter settings (see column 5, lines 39-41). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Finley's method of protection within a computer system and Brundrett's file encryption system with Hsu's computer system with transparent file transform services in order to prevent hackers from gaining access to the core operating system commands via embedded viruses [see **Finley**; column 1, lines 22-43] and to further provide the encryption system

with the flexibility of selecting algorithms in accordance with the user's needs for a particular file [see **Brundett et al**; column 1, line 63 to column 2, line 3].

Regarding claim 67, Hsu and Brundrett et al disclose everything claimed as applied above, (see claim 66), however, both fail to specifically teach a mechanism for invoking or running a virus scan program on the files executed within the computer system. Finley teaches a computer system in which user programs are executed in a location where embedded viruses can be detected transparent to the user (see column 3, line 51 to column 6, line 58). Finley teaches the security settings and the filter processors can be set by the operator. This allows the operator (user) the option to invoke security and/or filter settings (see column 5, lines 39-41). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Finley's method of protection within a computer system and Brundrett's file encryption system with Hsu's computer system with transparent file transform services in order to prevent hackers from gaining access to the core operating system commands via embedded viruses [see **Finley**; column 1, lines 22-43].

Regarding claim 74, Hsu teaches a computer system that uses a transparent file transform mechanism for encrypting and decrypting files (see column 3, line 14 to column 4, line 26 and column 6, line 1 to column 18, line 7). Hsu's preferred embodiment uses a file-oriented paradigm in providing the operating services on a UNIX operating system (see column 5, lines 46-48 and column 6, lines 44-45). The file transform mechanism provides transparent encryption/decryption services after receiving a change command to act on the file (see column 16, line 50 to column 17,

line 39 and Figure 5B.) Hsu fails to specifically teach selecting an algorithm from a plurality of algorithms to use on the file and validating (verifying) the encrypted data identifier. Brundrett teaches a file encryption system in which a user is allowed to select an algorithm from a plurality of algorithms and to encrypt using the selected algorithm (see column 10, lines 54-66). Brundrett also teaches validating (verifying) the integrity of the encrypted data (see column 16, lines 12-22). Hsu also fails to specifically teach a mechanism for invoking or running a virus scan program on the files executed within the computer system. Finley teaches a computer system in which user programs are executed in a location where embedded viruses can be detected transparent to the user (see column 3, line 51 to column 6, line 58). Finley teaches the security settings and the filter processors can be set by the operator. This allows the operator (user) the option to invoke security and/or filter settings (see column 5, lines 39-41). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Finley's method of protection within a computer system and Brundrett's file encryption system with Hsu's computer system with transparent file transform services in order to prevent hackers from gaining access to the core operating system commands via embedded viruses [see **Finley**; column 1, lines 22-43] and to further provide the encryption system with the flexibility of selecting algorithms in accordance with the user's needs for a particular file [see **Brundett et al**; column 1, line 63 to column 2, line 3].

Regarding claim 75, Hsu teaches a computer system that uses a transparent file transform mechanism for encrypting and decrypting files (see column 3, line 14 to column 4, line 26 and column 6, line 1 to column 18, line 7). Hsu's preferred

embodiment uses a file-oriented paradigm in providing the operating services on a UNIX operating system (see column 5, lines 46-48 and column 6, lines 44-45). The file transform mechanism provides transparent encryption/decryption services after receiving a change command to act on the file (see column 16, line 50 to column 17, line 39 and Figure 5B.) Hsu fails to specifically teach selecting an algorithm from a plurality of algorithms to use on the file and validating (verifying) the encrypted data identifier. Brundrett teaches a file encryption system in which a user is allowed to select an algorithm from a plurality of algorithms and to encrypt using the selected algorithm (see column 10, lines 54-66). Brundrett also teaches validating (verifying) the integrity of the encrypted data (see column 16, lines 12-22). Hsu also fails to specifically teach a mechanism for invoking or running a virus scan program on the files executed within the computer system. Finley teaches a computer system in which user programs are executed in a location where embedded viruses can be detected transparent to the user (see column 3, line 51 to column 6, line 58). Finley teaches the security settings and the filter processors can be set by the operator. This allows the operator (user) the option to invoke security and/or filter settings (see column 5, lines 39-41). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Finley's method of protection within a computer system and Brundrett's file encryption system with Hsu's computer system with transparent file transform services in order to prevent hackers from gaining access to the core operating system commands via embedded viruses [see **Finley**; column 1, lines 22-43] and to further provide the encryption system

with the flexibility of selecting algorithms in accordance with the user's needs for a particular file [see **Brundett et al**; column 1, line 63 to column 2, line 3].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Matthew B. Smithers
Matthew B Smithers
Primary Examiner
Art Unit 2134

November 17, 2002